CHAPTER 15

MEDIA SANITATION AND DISPOSAL

REVISED NOVEMBER 2019

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 15

MEDIA SANITATION AND DISPOSAL

1. PURPOSE. To define the requirements related to the sanitization of data from media, both digital and nondigital, prior to reuse or release from departmental control and define sanitation mechanisms with strength and integrity commensurate with the classification or sensitivity of the data.

2. SCOPE. The scope of this policy applies to any electronic information storage device or paper-based media containing sensitive or confidential data repurposed or transferred outside of the California Highway Patrol (CHP). This applies to all media including, but not limited to, embedded, removable, and/or portable memory storage (e.g., hard disk drives, CDs, DVDs, magnetic tape, floppy disks, memory cards, USB drives, smartphones, tablets, multifunction print devices, and digital cameras). This policy applies for all destinations including, but not limited to, surplus property, trash, recycling, donation, and off-site repair.

3. POLICY. Information Technology Section (ITS) is required to securely dispose of systems that store, process, or transmit sensitive data. Computer systems, electronic devices, and electronic media repurposed internally or transferred outside of the CHP, for any reason, must not contain sensitive or confidential data. When donating, selling, transferring, reissuing, or disposing of any device or removable media, care must be taken to ensure sensitive and confidential data cannot be retrieved or reconstructed. For example, if computers are surplused, any sensitive and confidential information stored on the machines must be thoroughly erased/wiped. In general, it is insufficient to delete the information, because it may remain on the medium. Department of Defense (DoD) compliant software that rewrites random data on the medium, preferably several times, must be used instead. Alternatively, the medium may be manually or electromagnetically destroyed.

a. If a device containing sensitive or confidential data requires repair by a nondepartmental employee but remains in our facility, the repair person must sign a CHP 110, Confidentiality Agreement. Approval must be obtained from the Department Information Security Officer (ISO) to release the device. The repair person must be informed in writing the system is only to be worked on by persons who have signed the CHP 110.

b. If a device containing sensitive or confidential data is removed from a CHP facility for repair, it must be sanitized using a Department ISO-approved utility or method prior to authorized release.

c. If a device containing sensitive or confidential data is sent outside the CHP for repairs and the unit is not repairable, the vendor must be instructed to return it to CHP for destruction.

NOTE: The Office of Primary Interest to which the device is assigned shall determine whether the device contains sensitive or confidential information. If ITS is a party to the repair process, ITS shall verify whether the device contains sensitive or confidential information.

4. MEDIA SANITIZATION AND DISPOSAL METHODS. Prior to disposal of any device or media containing sensitive or confidential data, the device or media must be sanitized using a Department ISO-approved utility. If the wiping process cannot be completed without error, the medium may be manually or electromagnetically destroyed to ensure the data cannot be retrieved or reconstructed.

5. PROCEDURES FOR DISPOSAL OF MEDIA.

a. Formal procedures for the secure disposal of media should minimize the risk of sensitive or confidential information leakage to unauthorized persons.

(1) If no longer required, the contents of any reusable media to be repurposed or removed from CHP should be made unrecoverable.

(2) Media containing sensitive or confidential information should be stored and disposed of securely and safely (i.e., by incineration or shredding), or erased.

(3) Destroy paper using crosscut shredders which produce particles that are one by five millimeters in size, or pulverize/disintegrate paper materials using disintegrator devices equipped with a 3/32-inch security screen.

(4) Destroy microforms (microfilm, microfiche, or other reduced-image photo negatives) by burning. When material is burned, residue must be reduced to white ash.

(5) Compact Discs, DVDs, magneto-optic disks, tape, hard drives, flash drives, etc., must be wiped or destroyed by pulverizing, crosscut shredding, or burning.

b. The following practices do NOT effectively remove or protect sensitive or confidential data on data storage media and should NOT be used:

(1) Reformatting. Most operating systems, including Microsoft Windows, store information on the hard drive in two areas – system and data. The system area contains information about where on the hard drive (in which sectors) the data is stored. The data area contains the actual data or files. When a hard drive is reformatted, the operating system normally overwrites the system information but does not overwrite the data area.

(2) Disk Imaging. Disk imaging is the copying of the entire contents of a hard drive, including its configuration settings and applications, to another hard drive. Since this does not overwrite the disk a sufficient number of times and does not guarantee overwriting of all of the data, it is not an acceptable method.

6. PROCEDURES FOR MEDIA SANITATION DOCUMENTATION. The ITS uses the following procedures to document and verify sanitation and disposal actions.

a. Control Objective. The Department tracks, documents, and verifies media sanitization and disposal actions.

b. Standard. Asset custodians will conduct media sanitation actions as follows:

(1) Receive media items to be sanitized on a timely basis and secure them at CHP Headquarters ITS Warehouse.

(2) Inspect media items for serviceability and ensure a completed CHP 266, Credit Memo - Equipment, was enclosed. All CHP 266s will be kept on file for future reference and retained per Department of General Services (DGS) Records Retention Schedule policies.

(3) Approved data wiping software will be used to ensure proper erasure of sensitive materials from storage medias is accomplished according to Statewide Administrative Manual, Section 5365.3, Media Disposal; National Institute of Standards and Technology Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations; and DoD 5220-22-M standards.

(4) Upon completion of the data clearing process, media items will be separated and determined to be serviceable for a future date, or unserviceable and prepared for survey and/or destruction.

(5) For serviceable items, recently wiped media will be reinstalled to previously attached devices, prepared for software imaging, and stored on standby replacement status at the ITS Warehouse.

(6) For unserviceable items, recently wiped media will be physically destroyed (if feasible), placed on pallets with proper labels, and shipped to DGS for final destruction/disposition.

(7) Some information technology devices with wiped media may be deemed as excess and will be sent to DGS and education-based nonprofit organizations (e.g., Computers for Classrooms) for distribution and/or future use.

ANNEX A

DEFINITIONS

1. DEFINITIONS.

a. Disposal. Disposal is the act of discarding media with no other sanitization considerations. This is most often done by recycling paper containing nonsensitive or confidential information but may also include other media.

b. Wiping. Wiping information is a level of media sanitization that would protect the confidentiality of information against a robust keyboard attack. Simple deletion of items would not suffice for wiping. Wiping must not allow information to be retrieved by data, disk, or file recovery utilities. It must be resistant to keystroke recovery attempts executed from standard input devices and from data scavenging tools. For example, overwriting is an acceptable method for wiping media. However, overwriting cannot be used for media that has been damaged or is no longer writeable. Destruction of the media must comply with Department of Defense 5220.22-M standards.

c. Destroying. Destruction of media is the ultimate form of sanitization. After media has been destroyed, it cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverizing, shredding, and melting.

d. Disintegration, Incineration, Pulverization, and Melting. These sanitization methods are designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or incineration facility with the specific capabilities to perform these activities effectively, securely, and safely.

e. Shredding. Shredders can be used to destroy flexible media, such as diskettes, once physically removed from their outer containers. The shred size of the refuse should be small enough to reasonably assure the information cannot be reconstructed.

f. Sensitive Information. Privileged or proprietary information only certain people are authorized to see, and is therefore not accessible to everyone. This includes personal information, protected health information, and confidential personal data.

g. Confidential Information. Information that uniquely identifies people (e.g., social security number, credit card number, driver's license number, bank account number).

THIS PAGE INTENTIONALLY LEFT BLANK